MIC
Ministry of Internal Affairs and Communications

Legal Points of Attention on Introducing DMARC

**Second Telecommunications Consumer Policy Division,
Telecommunications Business Department, Telecommunications Bureau,
Ministry of Internal Affairs and Communications (MIC)**

Overview of DMARC

1. Overview of DMARC

(1) The domain administrator declares a handling policy of e-mail transmitted under the domain name in the case of a failure in the domain authentication of the e-mail at the time of reception and discloses the e-mail address to which the report described in (3) below is to be sent.

(2) With consideration of the handling policy specified in (1), either one of the following processes shall be applied to the e-mail that has a failure in the Domain Keys Identified Mail and Sender Policy Framework (DKIM and SPF) authentication on the reception server side.

- Nothing is done: Delivered to the recipient as it is.
- Quarantine: Quarantined by indicating the failure in authentication (treated as a spam).
- Rejection: Deleted from the reception server (the recipient does not recognize the existence of the e-mail).

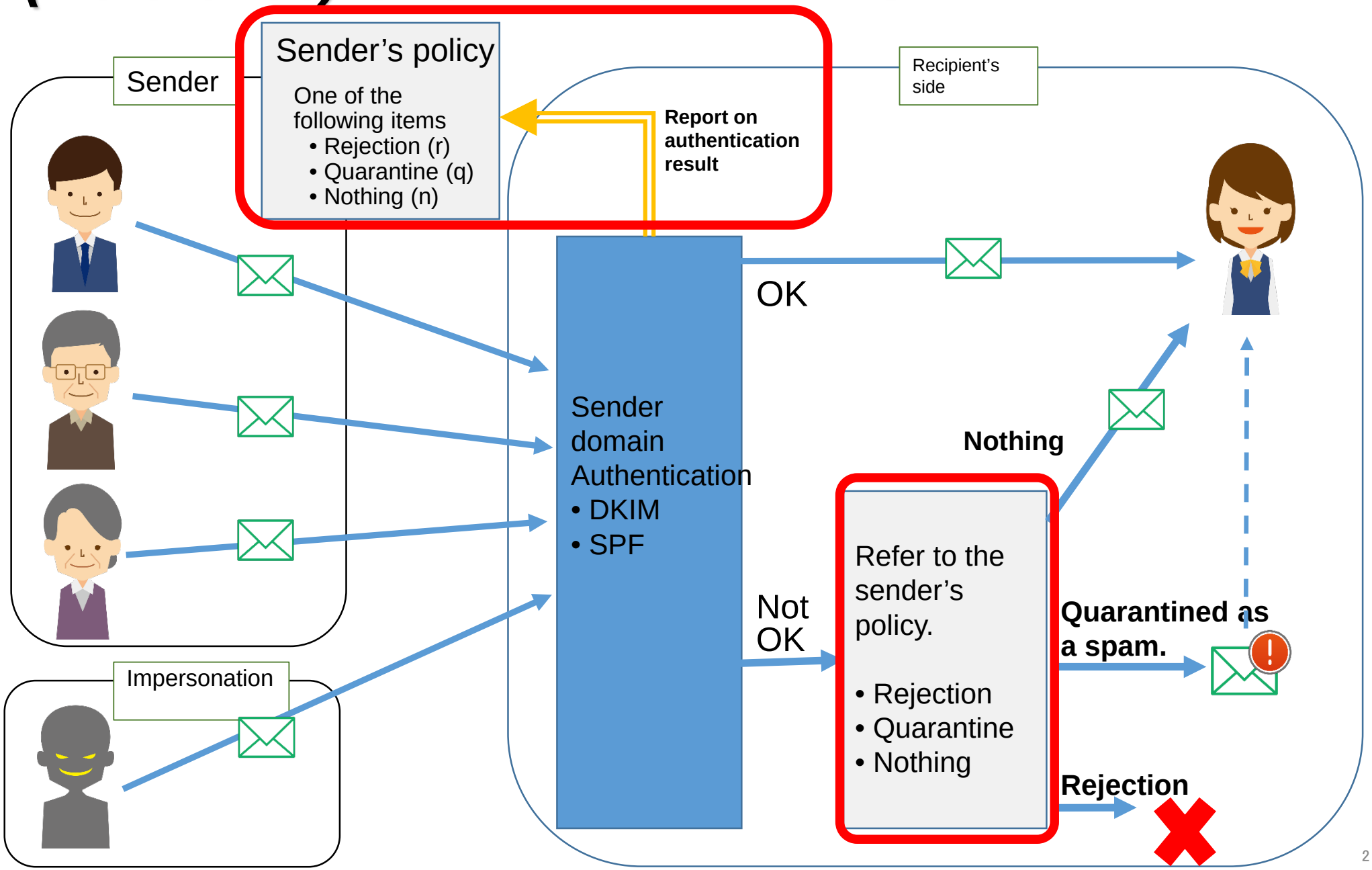
(3) The receiving server sends a report on the authentication result in (2) to the destination mail address specified by the sender domain administrator.

2. Legal Issue

Legally,

- Case (2) **is interpreted as an act of authenticating (checking) the transmission domain of the e-mail in the receiving server and taking certain measures if it cannot be authenticated.**
- Case (3) **is interpreted as an act of reporting information on a communications message that cannot be authenticated to the sender domain administrator or a party designated (e.g., the ISP, an analyst, etc.) by the sender domain administrator.** Both of them apparently can fall under **the act of infringing the confidentiality of communication prescribed in Article 4 of the Telecommunications Business Act**, and whether it is possible or not to apply them will be an issue.

(Reference) Overview of DMARC



Agreement of the parties on the introduction of DMARC

From the following reasons, **in principle, service providers are not allowed to have users abandon their confidential interests of communications in accordance with prior comprehensive agreements and such agreements are not understood as the constitution of the users' effective consent**: (1) Not complying with the nature of agreements (2) The subject of the consent is unclear.

If the following conditions are satisfied, however, it can be considered that the users' effective consent is acquired even if DMARC is provided on the basis of the comprehensive agreements.

1) The users can make setting changes by themselves at any time.
2) All other service conditions remain the same regardless of the presence or absence of the consent. (*1)
3) The subject and scope of the consent is clarified.
4) When sending a report on the result of domain authentication, neither the body nor subject of the e-mail is included in the content of the report. (*2)
5) An adequate explanation for the content of DMARC is given in advance (through procedures pursuant to the explanation of important matters prescribed in Article 26 of the Telecommunications Business Act). (* 3)

*1. There is no problem providing a filtering service including DMARC for a reasonable charge.
*2. None of the header information related to the content of the e-mail, including the main body and the subject header information, is contained.
*3. DMARC needs to explain the following points to each user clearly.
   1) Blocking based on the policy.
      • Information on blocking.
      • Information that the users cannot confirm the content of the e-mail that has been blocked.
   2) Making a report according to the request of the sender domain administrator.
      • Matters to be included in the report.
      • The fact that the above matter is sent to the destination designated by the sender.

(Reference) Conventional arrangements concerning the legitimate business conduct of domain authentication.

In order to say that an act falls under legitimate business conduct, it is necessary to satisfy: (1) The necessity for the purpose, (2) The validity of the conduct, and (3) The appropriateness of the means.

- Most e-mail messages from disguised senders are spams.
- It can reasonably be estimated that spams sent as means of advertisement are normally transmitted to a large number of people at one time.

Therefore, **it is possible to presume that e-mail spoofing a sending domain is sent to a large number of people at once**. **The provision of a filtering service** for the purpose of blocking such e-mail can be said **proper as long as the effective consent of the customers is obtained.**

Furthermore, the infringement of the secrecy of communication by the authentication is **limited to the transmission domain** as communication route information, **which does not exceed the limit necessary for filtering**. **Therefore, the act of authenticating the sending domain and labeling the result is recognized as a necessary and appropriate method for achieving the purpose of filtering**.

Accordingly, if the filtering service is provided with the effective consent of the customers, the act of domain authentication corresponds to a legitimate business act, which is the same in the act of domain authentication performed for the implementation of DMARC.